**Cryptanalysis of Vigenere Cipher Example**

**Ciphertext:**

CTMYR DOIBS RESRR RIJYR EBYLD IYMLC CYQXS RRMLQ FSDXF OWFKT

CYJRR IQZSM X

**Keyword: three-letters legal English word**

**Cryptanalysis – finding a key:**

**Step 1:**

Align a given ciphertext to the 3-letters keyword and color different colors ciphertext letters that corresponds to the first, second and third keyword letters.

**C T M Y R D O I B S R E S R R R I J Y R E**

**K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3**

**B Y L D I Y M L C C Y Q X S R R M L Q F S**

**K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3**

**D X F O W F K T C Y J R R I Q Z S M X**

**K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1 K2 K3 K1**

**Step 2:**

Find frequencies of the letters that correspond to the first letter of the keyword (the letters that should be taken in account will be in the first, fourth, seventh, etc positions – in my example these letters colored red), to the second and to the third letter of the keyword (second letter is colored green and third letter is colored blue)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Set 1:** **Red Letters -** | **Frequency** | **Set 2:****Green Letters**  | **Frequency** | **Set 3:****Blue Letters**  | **Frequency** |
| **C** | **2** | **T** | **2** | **M** | **2** |
| **Y** | **3** | **R** | **4** | **D** | **1** |
| **O** | **2** | **I** | **4** | **B** | **1** |
| **S** | **2** | **Y** | **2** | **E** | **2** |
| **R** | **3** | **L** | **1** | **R** | **3** |
| **B** | **1** | **S** | **2** | **J** | **1** |
| **D** | **2** | **M** | **1** | **L** | **2** |
| **M** | **1** | **F** | **1** | **Y** | **1** |
| **X** | **2** | **X** | **1** | **C** | **2** |
| **Q** | **1** | **W** | **1** | **Q** | **2** |
| **K** | **1** | **J** | **1** | **S** | **1** |
| **Z** | **1** |  |  | **F** | **2** |

**Step 3:**

Most frequent letters in the Set 1 is Y and R. Let’s start with Y.

You remember that most frequent letters of the English alphabet:

E, T, N, O, R, I, A, S

***Assumption:*** ciphertext Y is corresponded to one of the plaintext letters E, T, N, O, R, I, A, S. Use Vigenere table to find a possible key letter for each pair:

|  |  |  |
| --- | --- | --- |
| **Ciphertext letter** | **Possible plaintext letter** | **Corresponded key-word letter****Possible first letter of the keyword** |
| **Y** | **E** | **U** |
| **Y** | **T** | **F** |
| **Y** | **N** | **L** |
| **Y** | **O** | **K** |
| **Y** | **R** | **H** |
| **Y** | **I** | **Q** |
| **Y** | **A** | **Y** |
| **Y** | **S** | **G** |

**Most frequent letter in the Set 2 is R:**

|  |  |  |
| --- | --- | --- |
| **Ciphertext letter** | **Possible plaintext letter** | **Corresponded key-word letter****Possible second letter of the keyword** |
| **R** | **E** | **N** |
| **R** | **T** | **Y** |
| **R** | **N** | **E** |
| **R** | **O** | **D** |
| **R** | **R** | **A** |
| **R** | **I** | **J** |
| **R** | **A** | **R** |
| **R** | **S** | **Z** |

**Most frequent letter in the Set 3 is R**

|  |  |  |
| --- | --- | --- |
| **Ciphertext letter** | **Possible plaintext letter** | **Corresponded key-word letter****Possible third letter of the keyword** |
| **R** | **E** | **N** |
| **R** | **T** | **Y** |
| **R** | **N** | **E** |
| **R** | **O** | **D** |
| **R** | **R** | **A** |
| **R** | **I** | **J** |
| **R** | **A** | **R** |
| **R** | **S** | **Z** |

**Step 4:**

**Create a table of the possible key-word letters by writing side by side the last columns of the tables in Step 3**

|  |  |  |
| --- | --- | --- |
| **Corresponded key-word letter****Possible first letter of the keyword** | **Corresponded key-word letter****Possible second letter of the keyword** | **Corresponded key-word letter****Possible third letter of the keyword** |
| **U** | **N** | **N** |
| **F** | **Y** | **Y** |
| **L** | **E** | **E** |
| **K** | **D** | **D** |
| **H** | **A** | **A** |
| **Q** | **J** | **J** |
| **Y** | **R** | **R** |
| **G** | **Z** | **Z** |

**Step 5:**

Create all possible legal three-letters English words by choosing first letter from the first column, second from second column and third from third column.

For each possible keyword you will try to decipher the ciphertext and see if the plaintext makes sense.

 Possible keywords: FED, FEE, FEN, LEA, KEN, KEY, HER….

The answer: Deciphering the ciphertext with keyword KEY will give a plaintext:

**SPOON FEEDING IN THE LONG RUN TEACHES US NOTHING BUT THE SHAPE OF SPOON.**